**Amendments to the Specification:**

Please replace paragraph 0021 - 23 of the substitute specification with the following paragraphs:

--[0021] b) a group of units $Z^*_n$ with n as a composite integer;

[0022] ~~b)~~ c) a group of points on an elliptic curve over a finite body; and

[0023] ~~c)~~ d) a Jacobi variant of a hyperelliptic curve over a finite body.--

Please replace paragraph 0044 of the substitute specification with the following paragraph:

--[0044] g, p, $T_A$ $ID_A$, ~~gx~~ $g^x$ mod p, $H(g^x \text{ mod } p, pw, ID_A, T_A, \ldots)$,--